THE HONORABLE ROBERT S. LASNIK

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. PAIGE A. THOMPSON, Defendant.	No. CR19-159-RSL **REPLY IN SUPPORT OF DEFENDANT'S MOTION TO DISMISS COUNTS 2-8** Noted for January 10, 2022

The government's opposition falls flat. In the thirteen pages which constitute the government's opposition to defendant Paige Thompson's motion to dismiss Counts 2 through 8, the government wholly fails to address an issue central its prosecution of Ms. Thompson: namely, the fact that the actions with which Ms. Thompson is charged are akin to that of a novice white-hat hacker or security researcher. The government attempts to frame the issues by stating that it "is negligent for a person to leave the front door of his house wide open[, but] it is still illegal for a stranger to walk into that house and steal a television." (Gov't Opp. ("Opp.") at 5 (Dkt. No. 135).) But that is not what happened here and the government's analogy is wrongheaded for numerous reasons.

Had Ms. Thompson acted less erratically (rather than a person who has struggled her entire life with mental illness and her gender identity) and notified Capital One through its Responsible Disclosure Program (rather than alerting the information security community at large of the events in question), she surely would not have been charged. This is the kind of arbitrary and discriminatory prosecution that the Fifth

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

Amendment prohibits. If it is permitted to proceed, this prosecution will also chill free expression in violation of the First Amendment. Finally, the government is arguing for an expansion of the CFAA that will discourage white hat hackers from performing a necessary public service to the Internet community at large. The Court should dismiss the CFAA charges with prejudice.

I. The CFAA Counts Violate Ms. Thompson's Fifth Amendment Guarantee of Due Process of Law Because They Seek to Expand the CFAA to Common White Hat Hacking Behavior.

The government's claim that "everyone understands that intentionally intruding into someone else's computer systems and stealing information is illegal" is a self-serving and flawed attempt to reframe the issue. (*See id.* at 8.) The Court should reject the government's tort-based approach.

Numerous federal agencies, including the Department of Homeland Security, and companies actively engage the information security community to attempt to intrude into their computer systems and reward them with reports of success.[1] In such a context, the government's tort-based approach, which is not supported by *Van Buren*, offers no guidance whatsoever and leads to the kind of arbitrary and discriminatory

[1] *See, e.g.,* E. White, "'*Hack DHS' program to become permanent fixture at agency*," Federal News Network (Dec. 15, 2021), *available at* https://federalnewsnetwork.com/federal-newscast/2021/12/hack-dhs-program-to-become-permanent-fixture-at-agency/ (noting that DHS will pay monetary bounties for identification of vulnerabilities); B. Quarmby, *Polygon upgrade quietly fixes bug that put $24B of MATIC at risk*," CoinTelegraph (Dec. 30, 2021), *available at* https://cointelegraph.com/news/polygon-upgrade-quietly-fixes-bug-that-put-24b-of-matic-at-risk (stating that two white hat hackers were paid bounties for identifying "critical" vulnerabilities in blockchain contracts); M. Bryant, *'White hat' hacker behind $610m crypto heist returns most of money*, The Guardian (Aug. 13, 2021), *available at* https://www.theguardian.com/technology/2021/aug/13/white-hat-hacker-behind-610m-crypto-heist-returns-most-of-money (relating that a white hat hacker who took $610 million in crypto assets "for fun" and "to expose a vulnerability" was not prosecuted).

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

enforcement that is present here. *See Van Buren v. United States*, 141 S. Ct. 1648, 1652 (2021).

The government's tort-based approach appears to rest largely on the Ninth Circuit's decision in *Theofel v. Farey-Jones*, 359 F.3d 1066 (9th Cir. 2004), but that case is a civil Stored Communications Act ("SCA") case that predates *Van Buren*. (*See, e.g.,* Opp. at 1.) The Supreme Court firmly rejected a tort-based approach in its decision in *Van Buren*, leaving the dissent to cite the Second Restatement of Torts (as the government does here) to characterize the majority's decision as "at odds with basic principles of property law." 141 S. Ct. at 1664.

In any event, even though the case is inapposite, *Theofel* arguably supports Ms. Thompson's position here, since the Ninth Circuit recognized in that case that "[n]ot all deceit vitiates consent" in the context of alleged trespass and that the legal characterization of different "intrusions" may contain "fine and sometimes incoherent distinctions." 359 F.3d at 1073. While "fine and sometimes incoherent distinctions" may be completely acceptable in a civil case, they are *not* acceptable in a criminal statute. *See Kolender v. Lawson*, 461 U.S. 352, 357 (1983) (finding that penal statutes must "define the criminal offense with sufficient definiteness that ordinary people can understand what conduct is prohibited").

Given the lack of "minimal guidelines to govern law enforcement" in this type of prosecution under the CFAA, *Kolender v. Lawson*, 461 U.S. 352, 358 (1983)(citation omitted), it cannot be discerned whether the government is prosecuting Ms. Thompson because she does not "look like" or "sound like" others in the information security community. Or perhaps because she publicly disclosed Capital One's deficiencies with its handling of its own customers' personal information as opposed to a quiet, private notification that might have saved it from public embarrassment and derision. As such, this is precisely the situation where the Court ought to dismiss the CFAA counts as

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

violating the Fifth Amendment's due process guarantee. *See United States v. Nosal ("Nosal I")*, 676 F.3d 865, 863 (9th Cir. 2012) ("If there is any doubt about whether Congress intended [the CFAA] to prohibit the conduct in which [Nosal] engaged, then 'we must choose the interpretation least likely to impose penalties unintended by Congress.'")

II. The CFAA Counts Violate Ms. Thompson's First Amendment Freedom of Speech Because the Government's Interpretation of the CFAA is Not Narrowly Tailored to Meet a Significant State Interest.

The government's claim that "[t]here is no First Amendment right to hack other people's computers" demonstrates both a fundamental misunderstanding of Ms. Thompson's argument and the First Amendment. (*See* Opp. At 12.) The Court should reject this argument.

There is a First Amendment right inherent in expression through source code, which the CFAA may not infringe. *See, e.g., Sandvig v. Barr*, 451 F. Supp. 3d 73, 89 (D.D.C. 2020) (finding that CFAA should be interpreted narrowly to avoid violating the First Amendment right to free expression); *Junger v. Daley*, 209 F.3d 481, 485 (6th Cir. 2000) (holding computer source code protected by the First Amendment); *United States v. Bondarenko*, No. 217CR306JCMVCF, 2019 WL 2450923, at *10 (D. Nev. Jun. 12, 2019) (finding that source code, object code, and other computer software languages involve expression and are thus protected by the First Amendment). Notably, in *Sandvig*, the federal government refused to disavow criminal punishment under the CFAA where academic researchers intended to violate employment websites' terms of service to study racial and gender discrimination in hiring. 451 F. Supp. 3d 73. Similarly, in *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), the government affirmatively argued that a defendant's violation of a company's terms of service constituted a crime. Thus, the government's contention that the "CFAA criminalizes

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

hacking, not speech" should not be accepted. As *Sandvig* makes clear, the government has attempted to criminalize speech utilizing the CFAA, albeit unsuccessfully.

Under the First Amendment, where a law is content-neutral and only imposes reasonable restrictions on the time, place, or manner of protected speech, it is subject to intermediate scrutiny. *McCullen v. Coakley*, 573 U.S. 464, 477-79 (2014). Intermediate scrutiny requires the law to be "narrowly tailored to serve a significant governmental interest," *Packingham v. North Carolina*, 137 S. Ct. 1730, 1736 (2017) (citation omitted), and must "leave open ample alternative channels for communication of the information." *McCullen*, 573 U.S. at 477. In the context of criminal statutes, however, more careful scrutiny is required. *See Holder v. Humanitarian Law Project*, 561 U.S. 1, 28 (2010) (applying more rigorous scrutiny to criminal laws); *City of Houston v. Hill*, 482 U.S. 451, 459, (1987) ("Criminal statutes must be scrutinized with particular care.")

Here, the government's prosecution of Ms. Thompson runs afoul of the First Amendment because it does not limit application of the CFAA to the "breaking and entering" of protected computers, as originally contemplated by Congress. *See Sandvig*, 451 F. Supp. 3d at 86 (noting that the 1984 House Report on the CFAA "explicitly analogized the conduct prohibited by section 1030 to "forced entry"). Rather, the government seeks to criminalize white hat hacking, data mining, scraping, and access to publicly available resources on the Internet.

Ms. Thompson did not "break and enter," as the government claims. (*See* Opp. at 4.) Instead, she passed through an open gate and then allegedly copied information that was plainly accessible to her due to Capital One's malfeasance. In other circumstances, this behavior is rewarded with bug bounties and non-prosecution agreements.

Here, however, because Ms. Thompson did not privately notify Capital One of its error, and instead exercised her free speech to notify the community at large that

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

Capital One was inappropriately storing its customers' personal information in areas of AWS servers accessible to even the most novice hacker, she is facing criminal charges. This is an inappropriate extension of the CFAA that violates Ms. Thompson's First Amendment rights.

Moreover, neither the government's interpretation of the CFAA nor this prosecution is narrowly tailored to achieve its interest. As to the former, a reviewing court is required to interpret the statute narrowly. As to the latter, there are lesser measures available to both the government and the alleged victims. The government could seek to resolve this matter through a deferred prosecution,[2] and the alleged victims could pursue their claims in civil court and seek stay away orders.

III. The CFAA Counts Fail to State a Legally Cognizable CFAA Claim Because Her Access was Not Unauthorized as a Matter of Law.

The government's admissions in its response to Ms. Thompson's motion are fatal to its CFAA prosecution against Ms. Thompson. The government acknowledges it is proceeding against Ms. Thompson solely on the theory that she intentionally accessed a computer without authorization, *not* that she exceeded the authorization given by the computer system. (*See* Opp. at 3 [stating that Thompson is an "external" hacker, not an "internal" one].) In so doing, the government further admits that in accessing the computer, she "walked through a door that she knew had been left open by mistake[.]" (*Id.*)

[2] Deferred prosecutions are commonly granted by the government, but usually only with well-off corporate entities. For example, "[o]n December 11, 2012, HSBC Holdings and HSBC US entered into a deferred prosecution agreement in which they admitted laundering at least $881 million in drug-trafficking proceeds and agreed to pay $1.9 billion in forfeiture and fines." *Zapata v. HSBC Holdings PLC*, 414 F. Supp. 3d 342, 346 (E.D.N.Y. 2019).

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

That is not, and has never been held to be, a CFAA violation. If it were, then every white hat hacker in the world would be subject to criminal prosecution under the CFAA no matter how noble their motives or how much money they save governments and corporations. Ms. Thompson absolutely used the "access pathways and security credentials" of Capital One and AWS "as they were intended to be used," (Opp. at 3), which differentiates her case from those scant few cited by the government.

To support its argument, the government relies on two out of circuit cases and one Ninth Circuit case that are either not on point or easily distinguishable. (*See, e.g.,* Opp. at 1.) In the first, *United States v. Phillips*, 477 F.3d 215 (5th Cir. 2007), the defendant was convicted under the CFAA for a 14-month pattern of "brute force attacks" on university servers that (a) he was instructed to stop numerous times; (b) caused numerous crashes of the university systems over a period of months; and (c) which he used to knowingly take other people's personal information, including social security numbers. In finding there was sufficient evidence for his CFAA conviction, the Fifth Circuit stated that his "brute-force attack program was not an intended use" of the university's network and constituted "a method of obtaining unauthorized access to computerized data that he was not permitted to view or use." *Id.* at 220. The defendant's actions in *Phillips* were the quintessential "breaking and entering" hacking that Congress wanted to forestall with the passage of the CFAA. *See Sandvig*, 451 F. Supp. 3d at 86. Conversely, Ms. Thompson did not cause any of the allegedly affected AWS servers to become unresponsive nor did she use "brute force" to access them; rather, by the government's own admission, she used a publicly-available proxy server and publicly-known AWS commands to assume an IAM role within the servers that automatically gave her access to stored data.

United States v. Morris, the other case the government cites to, is so dated that it refers to the "Internet" as "the INTERNET." 928 F.2d 504, 505 (2d Cir. 1991). In any

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

event, in *Morris*, the defendant released a self-replicating "worm" to various known and unknown computer systems via mail and directory functions, which then rendered those computer systems unresponsive. *Id.* In support of the jury's verdict of guilt, the district court found that the defendant "did not use either of those features in any way related to their intended function" in that he "did not send or read mail nor discover information about other users[.]" *Id.* at 510. Ms. Thompson did not introduce a "worm" or any other sort of self-replicating virus into the AWS servers and the features she utilized on the AWS servers were used exactly how the alleged victims programmed them to work.

Lastly, in *Theofel*, the Ninth Circuit analyzed a "patently unlawful" subpoena issued under the SCA in a civil matter, not the CFAA, which makes any commentary about the CFAA in that opinion pure dicta. 359 F.3d at 1071. Even so, the off-handed comment that a "hacker could use someone else's password to break into a mail server and then claim the server 'authorized' his access" does not really address the situation here. *Id.* Ms. Thompson did not use someone else's password—the web application firewall gave her the security credentials automatically once she passed through the gate left open by the alleged victim entities.

To summarize, Ms. Thompson did not "break and enter" into any of the alleged victim's computer systems, as the government claims, nor is there any allegation that she caused any of the systems to become nonresponsive. By the government's own admission, Ms. Thompson walked through a port, Port 443, that was left "unlocked by mistake." (Opp. at 4.) In other words, the gate was down, and her alleged activity is protected. *See Van Buren*, 141 S. Ct. at 1659; *see Domain Name Comm'n Ltd. v. DomainTools LLC*, 449 F. Supp. 3d 1024, 1027 (W.D. Wash. 2020) (Lasnik, J.) (stating that whether access is authorized depends on the actions taken by the owner of the computer system).

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

Further, once inside the gate, she did not use another person's password or send "brute force" commands to gain any further access. Rather, the system granted her access (the IAM role) automatically once she executed a set of known commands because the system mistook her for an authorized visitor given the lack of protection on the door. (Opp. at 4 ["The internal server gave Thompson these credentials because it mistook her for an authorized internal user."]) That was not access to *all* the doors, and Ms. Thompson had no way to know what was behind the doors she was permitted access to until after the access was granted (unlike the defendants in *Phillips, Morris,* and even *Theofel,* whose end games were patently clear).

Put another way, Ms. Thompson's alleged actions utilized the AWS server features exactly how AWS and the alleged victim entities programmed them to work. Capital One and the other alleged victims *could* have configured their web application firewalls differently, which would have required Ms. Thompson to engage in the sort of "breaking and entering" that the CFAA criminalizes. But they did not. Although the authorization that was automatically granted to Ms. Thompson might have been, at best, a "mistake," it was authorization nonetheless. This precludes any criminal CFAA liability, and requires the dismissal of the CFAA counts.

IV. Conclusion

The defense wholeheartedly agrees with the government that "the context of the intrusion always matters." (Opp at 5.) Here, the context of Ms. Thompsons alleged intrusion, however, does *not* support multiple CFAA charges.

The government has not, and cannot, point to any case in which it has prosecuted an individual under the CFAA for using a proxy scanner and a series of otherwise innocuous, scripted commands, which are recognized and run by the computer server accessed because of its own internal settings (set by the alleged victim), under the CFAA. And, unless the government is willing to prosecute every white hat hacker who

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100

does the same (which it has not and never will do), the prosecution of Ms. Thompson is nothing but an arbitrary and discriminatory prosecution against a transgendered person with mental health issues.

For all of the above-stated reasons and in the underlying motion, the Court should dismiss Counts 2 through 8 with prejudice.

DATED: January 10, 2022

Respectfully submitted,

/s/ *Mohammad Ali Hamoudi*
MOHAMMAD ALI HAMOUDI
/s/ *Christopher Sanders*
CHRISTOPHER SANDERS
/s/ *Nancy Tenney*
NANCY TENNEY
Assistant Federal Public Defenders

/s/ *Brian Klein*
BRIAN KLEIN
/s/ *Melissa Meister*
MELISSA MEISTER
Waymaker LLP

Attorneys for Paige Thompson

FEDERAL PUBLIC DEFENDER
1601 Fifth Avenue, Suite 700
Seattle, Washington 98101
(206) 553-1100